Database Management System Evaluations

This module is the first of four modules that describe the use of the Trusted Database Interpretation (TDI) of the Trusted Computer System Evaluation Criteria (TCSEC) for database product evaluation and certification. This module presents the trusted database concepts outlined in the TDI. TDI Module Two describes various security policies which can be supported by a trusted database management system (DBMS). TDI Module Three describes various architectural approaches for building a trusted DBMS. TDI Module Four describes other database security issues that are not covered by the TDI but are important issues in database security, such as inference, aggregation, and database integrity.

Module Learning Objectives

This module provides a synopsis and explanation of the contents of the TDI. Upon completion of this module the student should:

1) be familiar with the organization and contents of the TDI.

2) understand the relationship between the TCSEC and the TDI and how to use the TDI.

3) understand the concept of TCB subsets and the conditions for evaluation by parts.

4) understand the three evaluation alternatives that are available based on the design choices the vendor made during the development of his trusted DBMS product.

5) understand which TCSEC requirements must be examined globally within composed TCBs and which requirements can be examined locally within individual TCB Subsets when determining compliance for a composite TCB.

Overview

During the initial phases of research into trust technology, secure DBMSs received far less attention than did secure operating systems. A major factor was the perception that one could not securely implement a trusted DBMS until trusted operating systems became available. Other security concerns included how to deal with inference and aggregation[1] in a multilevel system.

Research into trusted DBMSs (mostly theory) began during the 1970's and continues to the present day. In 1982 a database security workshop was held in Wood's Hole, Massachusetts which provided the basis for future database security issues. During the mid 1980's secure operating systems started becoming available which could provide a secure foundation for a trusted

1. Inference and Aggregation are described in detail in TDI Module Four.

DBMS. In June of 1986, the National Computer Security Center (NCSC) initiated an effort to address the evaluation of trusted DBMSs with an invitational workshop in Baltimore, Maryland. This group built on the efforts begun during the Wood's Hole meeting. During this workshop various database security issues were presented with different views on aggregation, inference, and how to secure a database.

Although many of these issues were still areas of research, it was obvious that trusted applications (e.g., DBMSs) were required to enforce security policies that are similar to those required of operating systems. An interpretation of the basic TCSEC criteria was needed to extend these security requirements to the unique architectures of DBMSs.

The Trusted Database Management System Interpretation (TDI) of the TCSEC was published in April 1991. The TDI is not a stand alone document, but instead is a document to be used in conjunction with the TCSEC. The TDI provides an interpretation of the TCSEC, allowing the TCSEC to be extended to trusted DBMSs.[2]

TDI Purpose

The TDI has been developed to provide a standard for trusted product vendors, a metric for trust evaluations, and a basis for acquisition specifications of trusted DBMS products.

The TDI was developed as a standard to guide developers in providing security features in their new and planned commercial DBMS products. In particular, the trust requirements stated in the TCSEC are interpreted for DBMS products. It is intended that a wide variety of systems satisfying these trust requirements will become widely available.

As an evaluation metric, the TDI provides a means with which to evaluate the degree of trust that can be placed in a DBMS for the secure processing of classified and other sensitive information. The TDI is used for both formal product evaluations and certification evaluations. Formal product evaluations, such as those performed by the NSA under the Trusted Product Evaluations Program, are performed on a computer product from a perspective that excludes the application environment. Certification evaluations assess whether appropriate security measures have been taken to permit a system to be used operationally in a specific environment.

Finally, the TDI may also be used as a basis for specifying DBMS security requirements in acquisition specifications. A detailed explanation of the rating structure unique to trusted applications is provided in Part 2 of Appendix B of the TDI. Understanding the meaning of the evaluation rating as well as the

---

2. The TDI is actually an interpretation of the TCSEC for any trusted application, however, DBMSs are used as an example throughout the TDI.

particular needs of the targeted environment are crucial to specifying the trust level required for a procurement.

System Compositions

Present day systems require multiple products (e.g., operating systems and DBMSs) and many times unique programs to implement the required functionality. In addition, today's complex systems are implemented using multiple computer systems which require communications such as local and wide area networks. Composition addresses how one integrates these products, computer systems, and networks in such a way that claims can be made about the security of the composed system.

There are two distinct classes of structures for reasoning about composition: partitioned and hierarchical [DTIN92]. A partitioned system is composed of cooperating, peer-entity elements. The responsibility for providing the required functions and enforcing the system security policy is allocated across the elements. The key characteristic is that elements must cooperate; the functions to be performed are implemented as separate, but interrelated, elements that communicate via mechanisms such as parameter- or message-passing. The *Trusted Network Interpretation* (TNI) addresses compositions of elements in this manner.

In contrast, the hierarchical structure is an ordered hierarchy characterized by dependency. Each element in the hierarchy "depends" on the lower (more primitive) elements for its correct functioning. With this structure there is a clear hierarchy of dependency[3]. Lower layers are more critical in that they must be correct as they can disrupt service of layers above them dependent upon their correctness.

The TDI addresses composition of systems with hierarchical components. However, the TDI was motivated for pragmatic reasons -- the need to evaluate new types of products that were planned for the marketplace and that would need to be "trusted" to implement the security policy defined in the TCSEC. In practice, vendors will typically submit their product for evaluation hosted on an existing platform which already has been evaluated. The question then is, "under what set of conditions is it possible to determine the global characteristics of the system as a result of the separate assessment of distinguishable parts of the system"? [DTIN92] The TDI calls the elements of the hierarchical structure "TCB Subsets" and the process "evaluation by parts".

Evaluation by Parts

The need for evaluation by parts evolved out of a realization that systems are rarely developed by a single manufacturer. The majority of present day systems are composed of a variety of hardware, software and firmware created

[3]. For a complete description of composition see [DTIN92].

by different manufacturers. Additionally, many systems are available on a wide variety of hardware platforms provided by different vendors. The difference between the software and firmware on these systems can be relatively minor.

In these cases considerable evaluation effort may be saved using a method of evaluating systems by parts. Such a method allows reuse of evaluation evidence from previously evaluated parts. A conservative approach towards such an evaluation technique is described in the TCB Subsets Section of the TDI (TC-4), and includes: a) a clear description of the parts considered for separate evaluation, b) a clear description of the conditions required for an evaluation by parts, and c) a general interpretation of the TCSEC requirements applicable to a system being evaluated by parts.

In order to build upon previous evaluation evidence, the parts of a complete system must be identified. The notion of the reference validation mechanism (RVM) allows us to argue for the delineation of parts of a system for separate evaluation.

A RVM (presented in TCSEC Module Six) has the following properties:

1) mediates all accesses between the subjects and objects under it's control;

2) is tamper resistant, and;

3) is simple enough to be analyzed.

Based on the ability of the parts to satisfy the RVM properties, the evaluated system's TCB can be logically divided into distinct parts or TCB subsets. These TCB subsets must satisfy the RVM properties on the basis of a stated access control policy. The subjects and objects specified in the TCB subset access control policy must be distinct. In other words, for subjects and objects in a system of multiple TCB subsets, each subject and object is a member of one and only one TCB subset.

TCB subsets are built upon either physical hardware machines (in the case that there are no TCB subsets more primitive) or abstract machines (in the case that the TCB subset is relying on more primitive TCB subsets to provide hardware resources, see figure 1). The only difference between the concept of TCB subsets and RVMs is that a TCB subset does not have to use the hardware resources directly. An evaluation of a system composed of a DBMS, the underlying operating system, and hardware may be divided into a DBMS TCB subset and a operating system TCB subset.

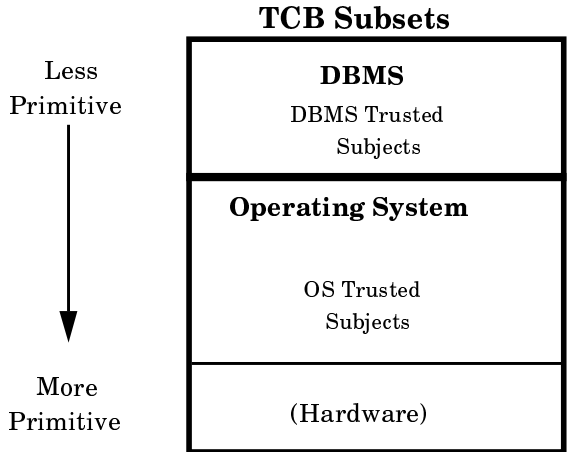

Figure 1: Example TCB Subsets

When these TCB subsets are properly constrained, considerable evaluation effort may be saved in future evaluations. Evaluation assurance gained from the evaluation of TCB subset(s) may be used in any subsequent evaluation to satisfy the requirements imposed upon the same TCB subset(s).

TCB Subset Constraints

There are three design choices available to developers of DBMSs. The simplest case is that of a monolithic system with a single TCB. This case applies to entire systems and requires no TCB subsetting. This type of system is evaluated against the requirements in the TCSEC.

The remaining two design choices are systems with distinct TCB subsets. These TCB subsets are identified by the TDI as either "meeting the conditions" or "not meeting the conditions". When a system has been internally structured to allow for the assessment of separate TCB subsets, a savings of evaluation effort may be possible. Below is a list of TCB subset conditions which, when met, allow for a system to be evaluated by parts. Each of these conditions is discussed in more detail in section TC-4.3 of the TDI.

1) The candidate TCB subset are identified,
2) The system policy is allocated among the candidate TCB subsets for enforcement,
3) Each candidate TCB subset includes all the trusted subjects with respect to the TCB subset's policies,
4) The TCB subset structure or architecture is explicitly described,
5) Each TCB subset occupies distinct subset-domains [see TDI, TC-4.3.5], and;

6) The more primitive TCB subsets provide support for the reference validation mechanism arguments for less primitive TCB subsets.

A system composed of TCB subsets meeting these conditions may save evaluation effort in future evaluations because local requirements (see section below) do not have to be reexamined for any previously evaluated TCB subsets. The entire composed TCB must still be examined with regard to all global properties the system must enforce. A system composed of TCB subsets which do not meet these conditions cannot be guaranteed the same savings of effort. The TDI cannot a priori describe the degree of evaluation effort that can be saved if these conditions are not met. Reuse of evaluation evidence for a composed TCB that does not meet these conditions is decided on a case by case basis. It is still possible that significant savings can be achieved depending on the nature of the violation and the system being evaluated.

Delineation of the Requirements

To support the reuse of evidence generated during previous evaluation efforts, the TDI divides the TCSEC into two sets of requirements, global and local. In a composed system, global requirements must be satisfied by each individual TCB subset as well as the system as a whole. Local requirements are those which can be met independently by individual TCB subsets. This designation allows the analysis of local requirements for a previously evaluated TCB subset to be reused in a subsequent evaluation.

For global requirements, evaluation effort is not conserved since compliance must be determined for each TCB subset, even if these TCB subsets have been previously evaluated as part of another system. For example, the global requirement for Audit is applied to each TCB subset. The Audit requirement requires a means for associating user identifications, which may differ between TCB subsets. Audit also requires that the security administrator be notified during the occurrence of certain security events. This notification ability must be satisfied regardless of the TCB subset in which the event occurred.

Previously evaluated TCB subsets do not need to be reevaluated to determine compliance with local requirements. For example, the local requirement of Object Reuse is applied separately to each TCB subset in a system being evaluated. Every object in the system belongs to exactly one TCB subset. Each TCB subset is responsible for meeting the object reuse requirements for its own objects.

The delineation of global and local requirements is summarized in table 1-1 below. The rationale for these distinctions is presented in Appendix B, section 7, of the TDI.

TCSEC Requirements	Global	Local
DAC		X
Object Reuse		X
Subject Sensitivity Labels	X	
Label Integrity		X
Exportation of Labeled Information		X
Subject Sensitivity Labels		X
Device Labels		X
MAC		X
I&A	X	
Trusted Path	X	
Audit	X	
System Architecture		X
domains for execution	X	
distinct address space	X	
System Integrity		X
Covert Channel Analysis	X	
Trusted Facility Management	X	
Trusted Recovery	X	
Security Testing	X	
Design Specification and Verification	X	
policy and subset model correspondence	X	
TCB interface and subset specification consistency	X	
Configuration Management		X
Trusted Distribution	X	
SFUG		X
Trusted Facilities Manual	X	
Test Documentation	X	
Design Documentation	X	
DTLS, FTLS, non-FTLS internals		X

Table 1-1: Global and Local Requirements

TDI Organization

The TDI is organized into two parts, a technical context (TC) and the interpreted requirements (IR). It also has two appendices which summarize

the interpreted TCSEC requirements and provide an overview of related topics.

Part I - Technical Context - presents general information about the evolution of trusted systems which are constructed of various parts. The entire concept of subsets, which allows the reference validation mechanism to be extended to trusted applications, is presented in this section. This extension provides the basis for being able to evaluate products which are built on portions of products which have been previously evaluated. By allowing the use of evidence from previous evaluations of the products, NSA intends to reduce the length of time required to evaluate the product.

Part II - Interpreted Requirements - provides the interpreted TCSEC requirements to be applied to systems composed of TCB subsets.

Appendix A - provides an easy reference of all the TCSEC requirements by class as they apply to DBMSs. Table 1-2 provides a listing of the TCSEC requirements interpreted for the TDI and a summary of their application to TCB subsets.

For each of the TCSEC requirements the table indicates whether the requirement has a specific interpretation for DBMSs and the applicability of the requirement to TCB subsets. Most requirements are applied to only one of the four categories: 'TCB subsets with a DAC policy', TCB subsets with a MAC policy', 'each TCB subset', or 'TCB as a whole', but Trusted Recovery in particular applies to each TCB subset and the TCB as a whole.

Requirements that apply to each TCB subset must be completely satisfied within each TCB subset (i.e., each TCB subset must meet the requirement). Requirements that apply to the TCB as a whole must be met by the combination of the TCB subsets and applies to the entire TCB.

TCSEC Requirements	Applies without interpretation	Applies to TCB subsets with a DAC policy	Applies to TCB subsets with a MAC policy	Applies to each TCB subset	Applies to the TCB as a whole
DAC	X	X			
Object Reuse	X			X	
Labels			X		
Label Integrity	X		X		
Export of Labeled Information	X		X		
Subject Sensitivity Labels	X				X
Device Labels	X		X		
MAC	X		X		
I&A	X				X
Trusted Path	X				X
Audit					X
System Architecture				X	
System Integrity	X			X	
Covert Channel Analysis	X				X
Trusted Facility Management	X				X
Trusted Recovery	X			X	X
Security Testing	X				X
Design Spec. and Verification				X	
Configuration Management	X			X	
Trusted Distribution	X				X
SFUG	X			X	
Trusted Facilities Manual	X			X	
Test Documentation	X				X
Design Documentation					X

Table 1-2: Application of TCSEC Interpreted Requirements to TCB Subsets

Appendix B - This appendix provides information on related issues. Sections include:

1) Perspective on Assurance

   This section emphasizes that only complete systems (i.e., those meeting all the TCSEC requirements for a given class) rather than subsystems or individual software packages will be evaluated against the TDI.

2) Procurement Options

   This section contains a description of how a system as a whole can satisfy a specific set of requirements for system security while relying on DBMSs of various levels of trust. The concept of 'balanced assurance' is introduced to provide flexibility in matching operational requirements with available products and system integration and development.

3) Alteration of Previously Evaluated TCB

   This section discusses how much new assurance evidence may be required for a previously evaluated TCB which is altered to provide services for a less primitive TCB Subset.

4) Satisfying RVM Requirements

   This section discusses the satisfaction of the requirement of support of RVM arguments in satisfying the conditions for evaluation by parts. Approval of this condition is reliant on an identified set of goals of the more primitive TCB subset and the ability to argue the RVM properties of the less primitive TCB subset based on those goals. Examples are used to illustrate the possible consequences of this step.

5) Subset Dependency

   This section discusses subset dependency issues illustrated with several examples. The issues presented are Use of Provided Objects, Mutually suspicious systems, use of remotely and locally provided functions, as well as a cautionary example of mutual dependency.

6) Tamper Resistance Arguments

   This section clarifies the evaluation by parts requirement that the individual TCB subsets demonstrate tamper resistance. The two aspects of this requirement, the ability of less primitive TCB subsets to maintain control of their objects, and the integrity of the policy and correctness critical data, are discussed in greater detail.

7) Rationale for Local and Global Requirements

   This section contains a discussion of the decision to make certain TCSEC requirements apply globally to a system with TCB subsets. For example, satisfaction of the trusted recovery requirement by individual TCB subsets is not sufficient. The trusted recovery capabilities of all TCB subsets

together must cooperate to satisfy the trusted recovery requirements for the TCB.

8) Content-Dependent and Context-Dependent Access Control

This section contains an acknowledgment of propositions for access control policies based solely on the context of the data or the context in which this data is accessed. The NSA recognizes these research directions, but does not currently take a stance as to the endorsement of any particular proposition.

9) Bulk Loading of a Database

Security issues concerning bulk loading and/or transfers of data from one database to another are discussed in this section.[4]

10) Local Analysis in System Assessment

This section discusses the issues surrounding the reuse of local analysis of TCB subsets for hosting and porting.

11) Rating More Complex Systems

The inaccuracy of applying a single evaluation rating to complex systems is discussed in this section.

Required Readings

The required readings are supplied as part of the source material for the module. These readings, and the module overview, provide all the material covered by the module test questions.

DTDI91 National Computer Security Center, *Trusted DBMS Interpretation of the Trusted Computer System Evaluation Criteria* (TDI), NCSC-TG-021, Version-1, April 1991.

The Introduction, the Technical Context and the Interpreted Requirements sections should be read in their entirety. They provide a good description of the history of database evaluation efforts, a logical method of accommodating their evaluation, and an interpretation of the TCSEC requirements for database evaluations. Appendix B contains brief discussions on several topics that may be of interest to the reader.

DTIN92 National Computer Security Center, *The Design and Evaluation of INFOSEC Systems: The Computer Security Contribution to the Composition Discussion*, Mario Tinto, C Technical Report 32-92, June 1992.

This document describes the composition problem which occurs when various systems and components are integrated together into a trusted

---

4. Although not mentioned in the TDI, the issue of label compatibility is important when considering bulk loading of a database. It is essential to ensure labels are interpreted and treated correctly.

system. The problem that arises is that it is difficult to argue about the security of the composed system. This paper describes the insights that have been gained in this area during the development of the TNI and TDI. It then describes how these two approaches, when combined together can be used to compose complex systems in such a way that it easier to argue about the security of the overall system through examination of its parts.

Other Related Readings

DBMS86 National Computer Security Center, Proceedings of the National Computer Security Center Invitational Workshop on Database Security, Baltimore, MD June 17-20 1986.

JGAR88 C. Garvey and A. Wu, *"ASD Views",* Proceedings of the Fourth Aerospace Computer Security Applications Conference, Orlando, Florida, December 1988, pp. 85-95.

JLUN88 T. F. Lunt, et. al., *"Final Report Vol. 1: Security Policy and Policy Interpretation for a Class A1 Multilevel Secure Relational Database System,"* Computer Science Laboratory, SRI International, Menlo Park, California, 1988.

JMCH88 J. McHugh and B.M. Thuraisingham, *"Multilevel Security Issues in Distributed Database Management Systems"*, Computer and Security, Vol. 7, No 4, Elsevier Advanced Technology Publications, August 1988, pp. 387-396.

JSCH87 W.R. Schockley and R.R. Schell, *"TCB Subsets for Incremental Evaluation,"* Proceedings of the Third Aerospace Computer Security Conference, Orlando, Florida, December 7-11, 1987, pp. 131-139.

JVET89 Linda Vetter and Bill Maimone, "*Multilevel Secure Database Management Systems"*, Proceedings of the Fifth Aerospace Computer Security Conference, Tucson, Arizona, 1989.

JWIN89 Helena Winkler-Parenty, *"Can You Trust Your DBMS?",* Database Programming and Design, July 1989.